

BUNDESREPUBLIK DEUTSCHLAND

EP 99/07019



PCT/EP 99/07019
item 17
REC'D 23 NOV 1999
WIPO EPO - DG 1
16. 11. 1999

EJU

(82)

Bescheinigung

09/555304

Die Philips Corporate Intellectual Property GmbH in Hamburg/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen"

am 5. August 1999 beim Deutschen Patent- und Markenamt eingereicht und erklärt, daß sie dafür die Innere Priorität der Anmeldung in der Bundesrepublik Deutschland vom 30. September 1998, Aktenzeichen 198 45 096.6, in Anspruch nimmt.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 06 F, G 06 K und H 04 L der Internationalen Patentklassifikation erhalten.

München, den 26. Oktober 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Nietiedt

Aktenzeichen: 199 36 890.2

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

Z u s a m m e n f a s s u n g

Um ein Verschlüsselungsverfahren, bei dem eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle (10) bzw. einem Register gespeicherten Daten ausgeführt wird, zur Verfügung zu stellen, welches eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert, wird vorgeschlagen dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle (10) in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.

Beschreibung

Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen

5

Technisches Gebiet

Die Erfindung betrifft ein Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle bzw. einem Register gespeicherten Daten 10 ausgeführt wird, gemäß dem Oberbegriff des Anspruchs 1.

Stand der Technik

In vielen Datenverarbeitungsgeräten dienen kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem 15 Gerät transportierte Daten. Die hierfür notwendigen Berechnungsoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei derartigen kryptographischen Berechnungen ist es oftmals notwendig, entsprechende Speicherbereiche bzw. Register des Datenverarbeitungsgerätes mit Operanden zu initialisieren. Bei den in diesem Zusammenhang verwendeten Daten bzw. 20 Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

25

Zur Berechnung der kryptographischen Algorithmen werden in den Datenverarbeitungsgeräten logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten 30 Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei kom-

plementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw.

5 Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (=Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann.

Bei einer aus der EP 0 482 975 B1 bekannten Speicherkarte mit Mikroschaltung und wenigstens einem Speicher, die an einem Datenverarbeitungsorgan angeschlossen ist, wobei das Datenverarbeitungsorgan von einem Datensignal von außerhalb der Karte gesteuert wird und als Antwort auf dieses Datensignal zu einem Zeitpunkt ein Befehlsendesignal abgibt, welches um eine vorbestimmte Dauer (T) bzgl. des Empfangs des Datensignals verzögert ist, wird zum Erhöhen des Schutzes die Zeitdauer (T) auf Zufallsbasis zeitlich variabel gewählt. Eine Kryptoanalyse auf der

Basis einer Stromänderung beim Beschreiben des Speichers kann dieses System jedoch nicht verhindern.

Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren der obengenannten Art zur Verfügung zu stellen, welches die obengenannten Nachteile beseitigen und eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert.

10 Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen gelöst.

Dazu ist es erfindungsgemäß vorgesehen, dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.

15 Dies hat den Vorteil, dass eine nicht vorbestimmte oder vorbestimmbare Vorinitialisierung vorliegt, welche aus Änderungen des Stromverbrauches beim Schreiben in die Speicherzelle keinen Rückschluß auf das in die Speicherzelle geschriebene Datenbitwort zuläßt. Beim Einschreiben von
20 Daten in derartig vorinitialisierte Speicherzellen ändert sich der Stromverbrauch lediglich abhängig von einer Differenz des Hamminggewichtes der eingeschriebenen Daten von der unbekannten Zufallszahl, so daß auch diese Differenz und damit die Änderung des Stromverbrauches zufällig und nicht vorherbestimmbar ist.

25 Bei der Umsetzung des Verfahrens bestehen verschiedene Möglichkeiten. Nach einer bevorzugten Vorgehensweise wird das auf Zufallszahlen basierende Bitwort von einem Rechenwerk in die Speicherzelle geschrieben. Alternativ wird das auf Zufallszahlen basierende Bitwort über eine direkte
30 Verbindung zwischen einer Zufallszahlenquelle und der Speicherzelle in letztere geschrieben.

Eine zeitliche Korrelation zwischen dem Einschreiben der Zufallszahl in eine Speicherzelle und der kryptographische Teiloperation wird dadurch vermieden, dass das auf Zufallszahlen basierende Bitwort zeitlich beabs. 5. standet vor der kryptographische Teiloperation in der Speicherzelle gespeichert wird.

Kurze Beschreibung der Zeichnungen

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen 10 näher erläutert. Diese zeigt in der einzigen Fig. ein Ablaufschema einer bevorzugten Ausführungsform eines erfindungsgemäßen Verfahrens.

Bester Weg zur Ausführung der Erfindung

Wie in der einzigen Fig. veranschaulicht, ist eine Speicherzelle 10 bzw. 15 ein Register zum Einschreiben bzw. Abspeichern von Daten x_i in Form eines Datenbitwertes über eine Verbindung 11 vorgesehen. Bevor jedoch der Operand x_i in die Speicherzelle 10 eingeschrieben wird, werden von einer Zufallszahlenquelle 12 Zufallszahlen erzeugt und über eine direkte Verbindung 14 in die Speicherzelle 10 eingeschrieben bzw. in dieser abgespeichert. Mit anderen Worten wird die Speicherzelle 10 mit einem Zufallswert r_i initialisiert. Alternativ zu der dargestellten Ausführungsform 20 kann das Einschreiben des Zufallswertes r_i auch über die Verbindung 11 von einem Rechenwerk erfolgen, welches zuvor den Zufallswert von der Zufallszahlenquelle 12 erhalten hat.

25

Der Zeitpunkt dieser Vorinitialisierung ist beliebig wählbar und erfolgt bevorzugt nicht unmittelbar vor der kryptographischen Operation. Zweckmäßigerweise erfolgt eine wiederholte Vorinitialisierung der Speicherbereich bzw. Register mit sich ändernden Zufallszahlen.

Werden die so vorinitialisierten Speicherbereiche bzw. Register im Zuge einer kryptographischen Operation mit Daten x_i geladen, ändert sich der Stromverbrauch nun lediglich abhängig von einer Differenz des Hamminggewichtes des Operanden x_i und des Hamminggewichtes der unbekannten Zufallszahl. Ausgehend von diesem zufälligen Differenzwert ist es nun nicht möglich, Angaben über die verwendeten Operanden bzw. Zwischenergebnisse abzuleiten.

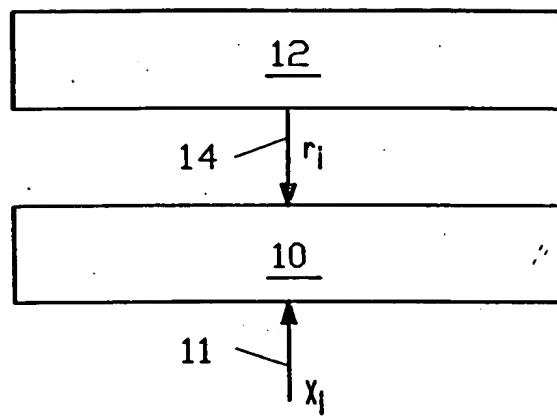
Patentansprüche

- 5 1. Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle (10) bzw. einem Register gespeicherten Daten ausgeführt wird,
dadurch gekennzeichnet, dass
10 vor dem Schreiben eines Datenbitwortes in eine Speicherzelle (10) in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.
2. Verschlüsselungsverfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
15 das auf Zufallszahlen basierende Bitwort von einem Rechenwerk in die Speicherzelle (10) geschrieben wird.
3. Verschlüsselungsverfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
20 das auf Zufallszahlen basierende Bitwort über eine direkte Verbindung zwischen einer Zufallszahlenquelle (12) und der Speicherzelle (10) in letztere geschrieben wird.
- 25 4. ~~Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,~~
dadurch gekennzeichnet, dass
das auf Zufallszahlen basierende Bitwort zeitlich beabstandet vor
30 der kryptographische Teiloperation in der Speicherzelle (10) gespeichert wird.

BEZUGSZEICHENLISTE

10	Speicherzelle / Register
5 11	Verbindung
12	Zufallszahlenquelle
14	Verbindung
X_i	Daten
T_i	Zufallswert

1/1



Fig

PHD 99-100

THIS PAGE BLANK (USPTO)